# BUNDESREPUBLIK DEUTSCHLAND



## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

**Aktenzeichen:** 100 63 934.8

**Anmeldetag:** 20. Dezember 2000

**Anmelder/Inhaber:** ROBERT BOSCH GMBH, Stuttgart/DE

**Bezeichnung:** Verfahren und Vorrichtung zur Überwachung und Abschaltung von Steuereinheiten in einem Netzwerk und Netzwerk

**IPC:** H 04 L, G 06 F

**Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.**

München, den 28. November 2001
**Deutsches Patent- und Markenamt**
**Der Präsident**
Im Auftrag



Dzierzon

A 9161
03/00
EDV-L

#4



U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

# CLAIM TO CONVENTION PRIORITY UNDER 35 U.S.C. § 119

| Docket Number: 10191/2117 | | | |
|---|---|---|---|
| Application Number: 10/026,026 | Filing Date: Dec. 20, 2001 | Examiner: To be assigned | Art Unit: 2184 |
| Invention Title: METHOD AND DEVICE FOR MONITORING AND DISCONNECTING CONTROL UNITS IN A NETWORK AND A NETWORK | | Inventor(s): Mathias HOMMEL | |

Address to:
Assistant Commissioner for Patents
Washington D.C. 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on

Date: 4/11/02 Reg. No. 22,490

Signature: R. Mayer
Richard L. Mayer

A claim to the Convention Priority Date pursuant to 35 U.S.C. § 119 of Application No. 100 63 934.8 filed in the German Patent Office on December 20, 2000 is hereby made. To complete the claim to the Convention Priority Date, a certified copy of the priority application is attached.

Dated: 4/11/02

By: D. Regn 35,952

By: _____
Richard L. Mayer (Reg. No. 22,490)

KENYON & KENYON
One Broadway
New York, N.Y. 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

R. 40057

20.12.00 Sy/Hx/Zj

ROBERT BOSCH GMBH, 70442 Stuttgart

# Verfahren und Vorrichtung zur Überwachung und Abschaltung von Steuereinheiten in einem Netzwerk und Netzwerk

## Stand der Technik

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Überwachung von Steuereinheiten in einem Netzwerk sowie ein entsprechendes Netzwerk, wobei jede Steuereinheit eine Sicherheitsfunktion zur Erkennung von Fehlern beinhaltet gemäß den Oberbegriffen der unabhängigen Ansprüche.

Eine solche Überwachung von Steuereinheiten in einem Netzwerk ist in der WO 90/09631 (US 5,499,336) beschrieben. Darin wird ein Verfahren zur Überwachung eines Computernetzwerks mit mindestens zwei über einen wenigstens zwei Leitungen umfassenden Datenbus verbundenen Teilnehmern, die jeweils ein Empfangs- und/oder ein Sendeteil aufweist, vorgeschlagen. Das Verfahren zeichnet sich dadurch aus, dass die Funktion des Datenbusses und/oder die Funktion der Teilnehmer mit Hilfe von Fehlererkennungssignalen durch mindestens einen Teilnehmer überwacht und das auf den jeweiligen Fehlerfall abgestimmte Notlaufmaßnahmen zur Einstellung von definierten Notlaufbetriebsarten ergriffen werden. Nach Ergreifung der ersten Notlaufmaßnahme wird geprüft, ob das Computernetzwerk fehlerfrei funktioniert. Wenn dies der Fall ist, wird die erste Notlaufmaßnahme aufrechterhalten und

auch damit die erreichte Notlaufbetriebsart. Sollten nach Eingreifen der ersten Notlaufmaßnahme weitere Fehler im Computernetzwerk auftauchen, wird die erste Notlaufmaßnahme zurückgenommen und die zweite Notlaufmaßnahme ergriffen. Wenn nunmehr keine weiteren Fehler auftauchen, wird der durch diese Maßnahme eingestellte Notlaufbetrieb, der Sondernotlauf aufrechterhalten. Erst wenn immer noch weitere Fehler auftauchen, werden die betroffenen Teilnehmer oder das gesamte Computernetzwerk abgeschaltet. Dabei ist der Einsatz einer Abschaltmatrix und damit einer differenzierteren Abschaltung mit verschiedenen Abschaltstrategien nicht gezeigt.

Daraus ergibt sich, dass bei einer Überwachung von mehreren Steuereinheiten in einem Netzwerk, also einem verteilten System, die oben beschriebene Situation dahingehend verbessert werden soll, dass eine differenziertere Abschaltung einzelner Steuereinheiten oder des gesamten Systems durch Einsatz einer Abschaltmatrix realisiert werden soll.

Vorteile der Erfindung

Dazu zeigt die Erfindung ein Verfahren und eine Vorrichtung zur Überwachung von Steuereinheiten in einem Netzwerk sowie ein entsprechendes Netzwerk, wobei jede Steuereinheit eine Sicherheitsfunktion zur Erkennung von Fehlern beinhaltet und jedem Fehler eine Überwachungsroutine zugeordnet ist, wobei eine Mehrzahl von Überwachungsroutinen zur Verfügung steht.

Vorteilhafter Weise ist der Sicherheitsfunktion eine Abschaltmatrix zugeordnet, welche nach Fehlern unterteilt ist, wobei entsprechend der vorhandenen Fehler der Abschaltmatrix wenigstens eine der Überwachungsroutinen abhängig von wenigstens einer ersten Bedingung aus der Mehrzahl von Überwachungsroutinen gewählt wird, wobei die Abschaltmatrix ver-

schiedene Abschaltstrategien enthält, wobei bei Erkennung wenigstens eines Fehlers durch die Überwachungsroutine abhängig von wenigstens der ersten und/oder wenigstens einer zweiten Bedingung eine der Abschaltstrategien des Netzwerks ausgeführt wird, wobei wenigstens eine Steuereinheit im Netzwerk abgeschaltet wird.

Weiterhin von Vorteil ist, dass die Erfindung eine Methode bereitstellt, um in verteilten Systemen, insbesondere SCS (safety critical systems) eine Abschaltung, differenziert insbesondere nach Fehlerursache, Betriebsart und Betriebszustand zu ermöglichen.

So gestattet es die erfindungsgemäße Methode zweckmäßigerweise die Fehlererkennung auf verschiedene Steuereinheiten eines Netzwerks zu verteilen und eine Abschaltung entsprechend der Abschaltmatrix insbesondere nach Fehler, Betriebsart (Funktion) und/oder Betriebszustand von den verschiedenen Steuereinheiten, insbesondere verteilt, durchführen zu lassen.

Dabei wird vorteilhafter Weise als erste und/oder zweite Bedingung zur Auswahl der jeweiligen Überwachungsroutinen und/oder der entsprechenden Abschaltstrategien entweder eine Fehlerkennung, eine Fehlerbeschreibung, eine Betriebsart (Funktion), ein Betriebszustand, je nach Steuereinheit bzw. Steuereinheiten für die Abschaltstrategie bzw. für die Überwachungsroutine, nach Fehlererkennungszeiten und/oder Anwendungstoleranzen bzw. Grenzen im Rahmen der Fehlererkennung ausgewählt.

Die genannte Sicherheitsfunktion läßt sich dabei zweckmäßigerweise wenigstens in die Teilfunktionen Sicherheitskern, Überwachungsroutinen und Abschaltstrategien unterteilen, wobei der Sicherheitskern auf allen Steuergeräten des Netzwer-

kes gleich ist. Vorteilhafter Weise umfasst der Sicherheitskern weiterhin wenigstens eine der Teilfunktionen Initialisierung, Fehlereintragung und Wiedergutprüfung.

In einer besonderen Ausgestaltung der Erfindung beinhaltet eine Steuereinheit des Netzwerkes koordinierende Funktion für alle anderen Steuereinheiten, wobei diese die zentrale Ausführung bezüglich wenigstens einer der folgenden Teilfunktionen der Sicherheitsfunktion zentral für das gesamte Netzwerk durchführt oder steuert: Initialisierung, Fehlereintragung, Wiedergutprüfung.

In einer weiteren besonderen Ausführungsform beinhaltet jede Steuereinheit einen individuellen Pool von Überwachungsroutinen, aus denen entsprechend der jeweils erkennbaren Fehler die Überwachungsroutinen wählbar sind, wobei dieser Pool bzw. diese Summe der Überwachungsroutinen für jede Steuereinheit unterschiedlich sind. Ebenso unterschiedlich sind in dieser besonderen Ausführungsform die jeweiligen Abschaltmatrizen der einzelnen Steuereinheiten, womit die Überwachung und die Abschaltstrategien verteilt auf alle Steuereinheiten des Netzwerkes durchgeführt werden.

Neben der völlig verteilen Ausführung der Überwachung und Abschaltung wird in einer weiteren besonderen Ausführungsform der Pool der Überwachungsroutinen, also die Überwachungsroutinen, die von jeder Steuereinheit wählbar sind, sowie die jeweilig wählbaren Abschaltmatrizen für jede Steuereinheit gleich oder wenigstens teilweise gleich vorgegeben, womit Überwachung und Abschaltstrategien redundant oder wenigstens teilweise redundant durchführbar sind.

Damit ergibt sich vorteilhafter Weise nicht nur die Möglichkeit, dass die Steuereinheit, die den Fehler erkennt, eine Abschaltung gemäß ihrer Möglichkeiten (Abschaltpfade, Ab-

schaltstrategien) durchführt, sondern auch die anderen Steuereinheiten, die sich noch im Netz befinden, können eine Abschaltung entsprechend ihrer Möglichkeiten (mögliche Abschaltstrategien, Abschaltpfade) aufgrund der Fehlererkennung der anfangs genannten Steuereinheit durchführen.

Weitere Vorteile und vorteilhafte Ausgestaltungen ergeben sich aus der Beschreibung und den Ansprüchen.

Zeichnung

Im weiteren wird die Erfindung anhand der in der Zeichnung dargestellten Figuren näher erläutert.

Dabei zeigt Figur 1 ein Netzwerk mit mehreren Steuereinheiten, welche über ein Bussystem verbunden sind.

Figur 2 zeigt beispielhaft für drei Steuereinheiten die Sicherheitsfunktion, insbesondere als Sicherheitssoftware SIS.

Figur 3 zeigt beispielhaft eine erfindungsgemäße Abschaltmatrix zur Ermittlung der jeweiligen Abschaltstrategie.

Beschreibung der Ausführungsbeispiele

Figur 1 zeigt ein Netzwerk 108 mit Steuereinheiten SE1 bis SEn 101 bis 103, welche über ein Bussystem 100 miteinander verbunden sind. Das Bussystem 100 kann dabei aus einem einzelnen Bus, beispielsweise einer Zweidrahtleitung, ebenso wie aus mehreren redundanten und/oder teilweise redundanten Datenbusen bestehen. Die Steuereinheiten, beispielsweise SE1, 101 beinhalten wenigstens einen Datenspeicher, in welchen Steuerdaten bzw. Steuerprogramme entsprechend der Steueraufgabe der jeweiligen Steuereinheit ebenso wie erfindungsgemäße Sicherheitssoftware SIS abgelegt ist. Daneben

kann zu diesem Zweck auch ein externes Speicherelement 104 über das Bussystem 100 angekoppelt Verwendung finden. Desweiteren sind am Datenbussystem 100 anzusteuernde Elemente 105, wie beispielsweise Aktuatoren oder Sensoren anbindbar. Solche Aktuatoren oder Sensoren insbesondere im Rahmen der Steueraufgabe des jeweiligen Steuergerätes bzw. der jeweiligen Steuereinheit können gleichermaßen wie für Steuereinheit SE2, 102 dargestellt, an diese direkt und nicht über Datenbussystem 100 angekoppelt werden, wie dies für ein beispielhaftes Sensorelement 106 sowie ein beispielhaftes Aktuatorelement 107 dargestellt ist. Die in der dargestellten Sensorankopplung bzw. Aktuatorankopplung verwendeten Doppelpfeile ebenso wie die Ankoppelpfeile an das Datenbussystem sollen durch ihre Bidirektionalität lediglich auf die entsprechenden Möglichkeiten hinweisen. Selbstverständlich ist gerade bei einer direkten Ankopplung der Elemente 106 und 107 an die Steuereinheit SE2 auch eine unidirektionale Verbindung beispielsweise vom Sensor 106 zur Steuereinheit SE2 bzw. von der Steuereinheit SE2 zum Aktuator 107 denkbar und möglich. Vor allem bei intelligenten Elementen 106 und 107 ist eine bidirektionale Anwendung denkbar.

Da die gezeigten Elemente 101 bis 105 bzw. 106 und 107 örtlich verteilt je nach Anwendung angeordnet sind spricht man bei Netzwerk 108 auch von einem verteilten System bzw. verteilten Systemen. Ein solches verteiltes System bzw. verteilte Systeme finden beispielsweise Anwendung in der Automobiltechnik, wo zum Beispiel mit SE2 ein Motorsteuergerät bzw. eine Motorsteuereinheit 102 mit SE1 eine Getriebesteuerung, also ein Getriebesteuergerät 101 dargestellt sind, welche beispielsweise über ein Datenbussystem, insbesondere einen CAN-Bus 100 miteinander verbunden sind. So können gerade im Automobilbereich beliebige Steuereinheiten über ein Datenbussystem 100 oder auch mehrere Datenbussysteme, welche über ein Gateway verkoppelbar sind, miteinander zu einem

Netzwerk 108 verbunden werden und müssen gerade im Sicherheitsfall als verteiltes System überwachbar sein. Neben dem Automobilbereich ist eine solche Anordnung noch für weitere Technikfelder, wie beispielsweise den Produktionsgüter-, insbesondere dem Werkzeugmaschinenbereich oder auch bei der Vernetzung anderer Systeme, wie Sicherheitssystemen denkbar.

Der prinzipielle Aufbau der bereits genannten Sicherheitssoftware SIS der einzelnen Steuereinheiten ist in Figur 2 beschrieben. Dabei wird im weiteren die Sicherheitssoftware SIS allgemein als Sicherheitsfunktion SIS bezeichnet, da eine Realisierung jenseits von Software, beispielsweise in Hardware, also festverdrahtet oder ähnliches, ebenso wie eine gemischte Lösung also in Software und festverdrahtet, möglich ist. Dazu sind die Steuereinheiten SE1, SE2 bis SEn im Rahmen ihrer Sicherheitsfunktion SIS schematisch dargestellt.

In einer ersten Ausführungsform ist die Sicherheitsfunktion SIS der einzelnen Steuereinheiten prinzipiell gleichartig aufgebaut. Die Sicherheitsfunktion SIS untergliedert in die Teilfunktionen bzw. Blöcke Initialisierung (1a, 1b, 1c), den Sicherheitsfunktionskern, SIS-Kern (2a, 2b, 2c), den Block Überwachungsprogramme (3a, 3b, 3c), welcher verschiedene Überwachungsroutinen enthält, die Abschaltlogik (4a, 4b, 4c), die Blöcke zur Eintragung des Fehlers in den Fehlerspeicher (5a, 5b, 5c) sowie zur Wiedergutprüfung im Fehlerfall (6a, 6b, 6c).

Die Initialisierung (1a, 1b bzw. 1c) richtet sich nach der jeweiligen Steuereinheit und wird beispielsweise einmal nach Start des Gesamtsystems, bzw. im Automobilbereich nach Zündung ein oder wenn eine beispielsweise abgeschaltete Steuereinheit wieder in Betrieb genommen wird, durchgeführt. Die Blöcke der Überwachungsprogramme (3a, 3b und 3c) sind die

jeweiligen Überwachungsroutinen, die insbesondere pro Abtastzeitschritt in diskreten, insbesondere digitalen Systemen einmal durchlaufen werden. Dabei ist jedem Fehler eine Überwachungsroutine zugeordnet, d.h. dass jede Überwachungsroutine wenigstens einen Fehler erkennen kann, insbesondere kann jede Überwachungsroutine genau einen Fehler erkennen.

Werden verschiedene Fehler in Fehlerarten klassifiziert, so gilt das Gleiche pro Fehlerart. Die jeweiligen Überwachungsroutinen können jeweils auf den verteilten Steuereinheiten des verteilten Systems, bzw. des Netzwerks, also in den Blöcken der Überwachungsprogramme (3a, 3b und 3c) gleich sein oder können für die jeweilige Steuereinheit spezifisch in der Zusammensetzung der einzelnen Überwachungsroutinen sein.

Die Abschaltlogik (4a, 4b, 4c) beinhaltet die programmtechnische Ausführung der Abschaltung und richtet sich nach der Hardware der Steuereinheit und der Ausführung der Abschaltstrategien bzw. Abschaltpfade, die die jeweilige Steuereinheit besitzt.

Dabei wird vorausgesetzt, dass die für die jeweiligen Fehlerüberwachungen notwendigen Daten, flags oder Sensorwerte, den betreffenden Steuereinheiten zur Verfügung stehen. Außerdem sollte die gewählte Abschaltung durch die jeweiligen Steuereinheiten sinnvollerweise physikalisch auch möglich sein, d.h. die beschriebenen Abschaltpfade sollten vorhanden sein.

Das bedeutet, dass sinnvollerweise nur solche Abschaltstrategien in einer Abschaltmatrix, die der jeweiligen Steuereinheit zugeordnet ist, vorgesehen sind, welche durch die jeweilige Steuereinheit aufgrund der vorgegebenen Abschaltpfade auch realisierbar ist, bzw. dass bei Vorgabe von Ab-

schaltstrategien das Vorhandensein der notwendigen Abschaltpfade kontrolliert, bzw. die notwendigen Abschaltpfade eingerichtet werden.

Eine Eintragung des Fehlers in den Fehlerspeicher (5a, 5b, 5c) erfolgt, wenn aufgrund der Überwachungsroutinen ein Fehler erkannt wurde, wobei eine Abschaltung eingeleitet wird oder bereits wurde und eingeleitet ist.

Diese Fehlereintragung ist ebenso wie die Wiedergutprüfung (6a, 6b und 6c) bei den Steuereinheiten 2 bis n optional, wenn im Rahmen einer zweiten besonderen Ausführungsform, beispielsweise Steuereinheit SE1, als koordinierendes Steuergerät eingesetzt ist. Gibt es, wie in dieser besonderen Ausführungsform, eine koordinierende Steuereinheit, beispielsweise SE1, welche die Initialisierung der verschiedenen Steuereinheiten verfolgt, so nimmt diese auch allein den Eintrag des Fehlers in den Fehlerspeicher vor und organisiert im Fehlerfall die Wiedergutprüfung. Dabei richtet sich die Initialisierung dann ebenso nach der jeweiligen Steuereinheit und wird auch nach Start des Gesamtsystems, oder wenn die koordinierende Steuereinheit eine abgeschaltete Steuereinheit wieder in Betrieb nimmt, durchgeführt. Die Initialisierung kann dann steuereinheitindividuell ablaufen und Initialisierungsschritte, welche das Kommunikationssystem, also den oder die Datenbusse, und/oder das Gesamtsystem betreffen sind zentral durch die koordinierende Steuereinheit ausführbar.

In jedem Fall sind aber die Teilfunktionen SIS-Kern, Überwachungsprogramme und Abschaltung, bzw. Abschaltstrategien, als Teilfunktionen der Sicherheitsfunktion SIS für alle Steuereinheiten des Netzwerks gleich.

Je nach Abschaltart bzw. Abschaltstrategie (später erläutert im Rahmen der Abschaltmatrix) kann eine Wiedergutprüfung erfolgen, wenn der Anlaß zum Auslösen des Fehlers nicht mehr besteht, was auch im Rahmen der Wiedergutprüfung festgestellt werden kann. War der Auslöser beispielsweise eine erhöhte Temperatur oder eine zu niedrige Batteriespannung, erfolgt die Wiedergutprüfung beispielsweise, wenn eben diese erhöhte Temperatur oder die zu niedrige Batteriespannung nicht mehr vorliegt. Gleichermassen kann die Wiedergutprüfung nach Ablauf einer vorgebbaren oder variablen Zeit nach Fehlererkennung erfolgen. In jedem Fall wird bei Start des Gesamtsystems, insbesondere bei jedem Zündung ein, bzw. Betätigung des Startschalters des Fahrzeugs eine Wiedergutprüfung durchgeführt, um die fehlerfreie Funktionsweise der Steuereinheiten des verteilten Systems nachzuweisen.

Der SIS-Kern (2a, 2b, 2c) ist ein Programmteil, bzw. eine Teilfunktion, welche in allen Steuereinheiten völlig identisch und somit austauschbar ist. Die Funktion des SIS-Kerns besteht im wesentlichen darin, dass aus der noch zu beschreibenden Abschaltmatrix nach einem weiter unten beschriebenen Algorithmus die Abschaltstrategie gewählt wird, beispielsweise abhängig vom jeweiligen Fehler von der jeweiligen Steuereinheit, von der Betriebsart und/oder vom Betriebszustand. Somit wird der SIS-Kern identisch auf allen im Netz befindlichen Steuereinheiten abgearbeitet. Dabei sucht dieser SIS-Kern sich aus der vollständigen (für das Gesamtsystem, oder bezüglich der Abschaltmatrix zusammengefasster Teile/Steuereinheiten des Gesamtsystems) oder nur der für die jeweilige Steuereinheit relevanten Abschaltmatrix, die im betrachteten Abtastschritt zutreffende Überwachungsroutine heraus, stößt diese an bzw. führt diese durch.

Im Fehlerfall wird durch den SIS-Kern mit Hilfe der Abschaltmatrix, insbesondere die nach Betriebszustand, Be-

triebsart oder Steuereinheit abhängige Abschaltart, bzw. Abschaltstrategie, differenziert ausgewählt und angestoßen bzw. durchgeführt.

Die Überwachungen können somit verteilt durchgeführt werden, d.h. teilweise oder völlig redundant oder lokal in einem völlig anderen Steuergerät ablaufen. D.h. nicht nur das Steuergerät, welches den Fehler erkennt, sondern auch die anderen im Netz befindlichen Steuergeräte können eine Abschaltung gemäß ihrer Möglichkeiten (Abschaltpfade, Abschaltstrategien) durchführen.

Um die Funktion des SIS-Kerns genauer beschreiben zu können, ist es notwendig, den prinzipiellen Aufbau der Abschaltmatrix zu erläutern, wie dies in Figur 2 dargestellt ist. Die Abschaltmatrix in Figur 2 besteht aus verschiedenen Spalten. Jede Zeile ist für einen speziellen Fehler zuständig. In der ersten Spalte 10 ist die Fehlernummer des jeweiligen Fehlers, bzw. dessen Fehlerkennung, abgespeichert. In der Spalte 12 ist eine Kurzbeschreibung des jeweiligen Fehlers, etwa für Fehleraufschriften oder ähnliches, abgelegt. Beispielhaft ist hier wieder die zu kleine Batteriespannung oder die zu große Temperatur gewählt. In der Spalte 11 sind die Betriebszustände binär kodiert, in denen die jeweiligen Überwachungen durchgeführt werden sollen. Ein Betriebszustand kann dabei zum Beispiel Initialisierung der Steuereinheit, der Normalbetrieb bei Fahrt, Normalbetrieb im Stillstand des Fahrzeugs, aktiv oder passiv, und so weiter sein.

Die jeweilige Überwachung wird im jeweiligen Betriebszustand durchgeführt, wenn an der entsprechenden Stelle beispielsweise eine Eins („1") anstatt einer Null („0") steht, also die entsprechende Stelle irgendwie markiert bzw. gekennzeichnet ist. In der Spalte 13 sind die Steuereinheiten, insbesondere ebenfalls binär, kodiert, in denen die Überwa-

chungsroutinen zum jeweiligen Fehler ablaufen sollen. Wenn an der entsprechenden Stelle wieder beispielsweise Eins anstatt einer Null steht, dann wird in dem jeweiligen Steuergerät, bzw. der Steuereinheit, die zum Fehler gehörende Überwachungsroutine ausgeführt.

In den Spalten 14 und 15 sind m Erkennungszeiten T1 bis Tm und n Grenzen G1 bis Gn mit m,n > 1 beliebig, aber fest, für die Fehlererkennung der Fehler abgelegt. Diese speziellen Matrixelemente können ausgefüllt sein, müssen es aber nicht. Bei umfangreichen Algorithmen ist es selbstverständlich, dass die jeweiligen Zeiten, Grenzen und Faktoren der Überwachung in der Überwachungsroutine selbst untergebracht sind, bzw. von dieser selbst aufgerufen werden.

In der letzten Spalte 17 sind die Abschaltarten der einzelnen Fehler abhängig von der Funktion, bzw. vom gerade aktiven Prozess, eingetragen. Dabei ist beispielsweise ein Unterschied denkbar, ob gerade beispielsweise ABS aktiv ist oder beispielsweise ABS und ASR und ESP oder auch ein aktiver Lenkeingriff durchgeführt wird sowie eine variable Lenkübersetzung ständig aktiv ist. Gleiches gilt im Rahmen der Motorsteuerung, Getriebesteuerung oder anderer, insbesondere fahrzeugspezifischer Funktionen.

Je nach Vorliegender Betriebsart/Funktion oder auch Kombination der Funktionen/Betriebsarten wird bei gleichem Fehler (hier gleiche Zeile in der Abschaltmatrix) unter Umständen eine andere Abschaltung durchgeführt, also eine andere Abschaltstrategie gefahren. Die Matrixelemente der Abschaltmatrix, die in Figur 2 in Spalte 17 bzw. 19 mit A1, A2, A3 und A4, bzw. A5 und A6, bezeichnet sind, bestimmen die Abschaltstrategie Spalte 19, bzw. Abschaltart, deshalb wurde dies eingangs als differenzierte Abschaltung bezeichnet. Als Beispiel für verschiedene Abschaltstrategien werden nun ge-

nannt: Sofortabschaltung, Abschaltung nach Regelungsende, Abschaltung bei Fahrzeugstillstand, Abschaltung aber Wiederinbetriebnahme wenn die Abschaltbedingungen nicht mehr vorliegen, Abschaltung einzelner Steuereinheiten oder des gesamten Netzwerks und so weiter.

Dabei kann wie erwähnt mittels Block 18 auch eine Kombination verschiedener Funktionen/Betriebsarten ausgewertet und zu einer bestimmten Abschaltstrategie verknüpft werden, wie gestrichelt angedeutet, wobei Block 18 optional ist und bei fehlendem Block 18 eine eins zu eins Zuordnung der Funktionen/Betriebsarten zu den Abschaltstrategien abhängig vom Fehler erfolgt.

Der SIS-Kern (2a, 2b, 2c) hat die Aufgabe, in jedem Abtastschritt für die jeweilige betroffene Steuereinheit die abhängig von den Spalten 11 und 13 zutreffende Überwachungsroutinen aufzurufen. Die Gesamtheit, also die Mehrzahl der in der jeweiligen Steuereinheit zur Verfügung stehenden Überwachungsroutinen, ist mit Überwachungsprogrammen, also 2a, 2b, 2c bezeichnet. Diese Routinen können einerseits individuell unterschiedlich oder gleich in jeder Steuereinheit als Mehrzahl der Überwachungsroutinen vorliegen oder auch zentral in einem zentralen Speicherelement als Mehrzahl aller Überwachungsroutinen abgelegt sein. Dabei können den Überwachungsroutinen die notwendigen Angaben, insbesondere aus Spalte 14 und 15, mit übergeben werden.

Im Falle eines Fehlers, der durch die Überwachungsroutine(n) festgestellt wird, wird abhängig von Spalte 10 und Spalte 17 bzw. 19 die definierte Maßnahme zur Fehlerbehandlung, also Abschaltung, von 4a, 4b, 4c ausgewählt und eingeleitet. Der SIS-Kern ist auf allen Steuereinheiten identisch. Die Abschaltmatrix kann in allen Steuereinheiten identisch sein, es genügt jedoch die für die jeweilige Steuereinheit rele-

vanten Teile in der jeweiligen Steuereinheit selbst abzubilden gemäß Spalte 13. Überwachungen können, abhängig von Spalte 13, auch doppelt, also redundant, auf verschiedenen Steuereinheiten ablaufen.

Wenn es ein koordinierendes Steuergerät, eine koordinierende Steuereinheit gibt, wie vorab genannt, beispielsweise SE1, wird bei Fehlerentdeckung durch zum Beispiel Steuereinheit SE 2 die Fehlernummer gemäß Spalte 10 an Steuereinheit 1 SE1 weitergegeben und Steuereinheit SE2 und/oder SE1 schaltet gemäß Spalte 17 bzw. 19, also den dort vorgegebenen Abschaltstrategien, ab.

Dabei kann über den Block 18 wie beschrieben auch eine Verknüpfung einzelner Funktionen mit daraus resultierender Abschaltstrategie in 19 erfolgen.

Dabei können aus Sicherheitsgründen die Abschaltpfade verschieden sein.

Steuereinheit 1 SE1 nimmt den Eintrag in den Fehlerspeicher vor und organisiert die Wiederinbetriebnahme der Steuereinheit SE2 und/oder des Gesamtsystems.

Gibt es keine koordinierende Steuereinheit, werden die Fehlernummern, bzw. Fehlerkennungen nicht ausgetauscht und jede Steuereinheit schaltet gemäß Spalte 17 bzw. der vorgegebenen Abschaltstrategien 19 ab, und nimmt den Eintrag in den Fehlerspeicher und die Wiederinbetriebnahme, bzw. Wiedergutprüfung, selbst vor, im Zweifelsfall erst wieder beim Start des Gesamtsystems, insbesondere bei Zündung ein.

Das in der Beschreibung geschilderte Verfahren ist dabei als Programm oder Programmprodukt auf einem Datenträger, wie ROM, insbesondere CD-ROM, EPROM, Diskette, Flash-EPROM, RAM,

usw. abspeicherbar und Einbringen und Auslesen auf einer Steuereinheit ausführbar. Dabei werden dann Schritte des Verfahrens gemäß der Beschreibung in der Steuereinheit bzw. dem verteilten System ausgeführt, weshalb auch dieses Programm oder Programmprodukt durch welches das erfindungsgemäße Verfahren ausgeführt wird Gegenstand der Erfindung ist.

20.12.00 Sy/Hx

ROBERT BOSCH GMBH, 70442 Stuttgart

Ansprüche

1. Verfahren zur Überwachung von Steuereinheiten in einem Netzwerk, wobei jede Steuereinheit eine Sicherheitsfunktion zur Erkennung von Fehlern beinhaltet, wobei jedem Fehler eine Überwachungsroutine zugeordnet ist und eine Mehrzahl von Überwachungsroutinen zur Verfügung steht, wobei der Sicherheitsfunktion eine Abschaltmatrix zugeordnet ist, welche nach Fehlern unterteilt ist, wobei entsprechend der vorhandenen Fehler der Abschaltmatrix wenigstens eine der Überwachungsroutinen abhängig von wenigstens einer ersten Bedingung aus der Mehrzahl von Überwachungsroutinen gewählt wird, wobei die Abschaltmatrix verschiedene Abschaltstrategien enthält und dass bei Erkennung wenigstens eines Fehlers durch die Überwachungsroutine abhängig von wenigstens der ersten und/oder wenigstens einer zweiten Bedingung eine der Abschaltstrategien im Netzwerk ausgeführt wird, wobei wenigstens eine Steuereinheit im Netzwerk abgeschaltet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass als erste und/oder zweite Bedingung wenigstens eine der folgenden ausgewertet wird:

- Fehlerkennung (10)
- Fehlerbeschreibung (12)

- Betriebsart (17)
- Betriebszustand (11)
- Steuereinheit für Abschaltstrategie (19)
- Steuereinheit für Überwachungsroutine (13)
- Fehlererkennungszeiten/Erkennungszeiten (14)
- Anwendungstoleranzen oder Grenzen (15)

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Sicherheitsfunktion sich wenigstens in die Teilfunktionen Sicherheitskern, Überwachungsroutinen und Abschaltstrategien unterteilt, wobei der Sicherheitskern auf allen Steuereinheiten des Netzwerkes gleich ist.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass weiterhin wenigstens eine der folgenden Teilfunktionen in der Sicherheitsfunktion enthalten ist:
- Initialisierung
- Fehlereintragung
- Wiedergutprüfung

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, das eine Steuereinheit des Netzwerkes koordinierende Funktion für alle anderen Steuereinheiten hat bezüglich wenigstens einer der folgenden, in der Sicherheitsfunktion dieser einen Steuereinheit enthaltenen Teilfunktionen:
- Initialisierung
- Fehlereintragung
- Wiedergutprüfung

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungsroutinen, die von jeder Steuereinheit wählbar sind entsprechend der jeweils erkennbaren Fehler,

sowie die jeweiligen Abschaltmatrizen der Steuereinheiten für jede Steuereinheit unterschiedlich sind und damit die Überwachung und die Abschaltstrategien verteilt auf alle Steuereinheiten des Netzwerkes durchgeführt werden.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Überwachungsroutinen, die von jeder Steuereinheit wählbar sind entsprechend der jeweils erkennbaren Fehler sowie die jeweiligen Abschaltmatrizen der Steuereinheiten für jede Steuereinheit gleich oder teilweise gleich sind und damit die Überwachung und die Abschaltstrategien redundant oder teilweise redundant durchführbar sind.

8. Vorrichtung zur Überwachung von Steuereinheiten in einem Netzwerk, wobei Mittel mit Sicherheitsfunktion in jeder Steuereinheit zur Erkennung von Fehlern enthalten sind, wobei jedem Fehler eine Überwachungsroutine zugeordnet ist, wobei eine Mehrzahl von Überwachungsroutinen zur Verfügung steht und den Mitteln mit Sicherheitsfunktion eine Abschaltmatrix zugeordnet ist, welche nach Fehlern unterteilt ist, wobei weitere Mittel enthalten sind, welche entsprechend der vorhandenen Fehler in der Abschaltmatrix wenigstens eine der Überwachungsroutinen abhängig von wenigstens einer ersten Bedingung aus der Mehrzahl von Überwachungsroutinen auswählen, wobei die Abschaltmatrix weiterhin verschiedene Abschaltstrategien enthält und dass die weiteren Mittel bei Erkennung wenigstens eines Fehlers durch die ausgewählte Überwachungsroutine abhängig von wenigstens der ersten und/oder wenigstens einer zweiten Bedingung eine der Abschaltstrategien im Netzwerk ausführen, wobei wenigstens eine Steuereinheit im Netzwerk abgeschaltet wird.

9. Netzwerk mit mehreren Steuereinheiten, wobei jede Steuereinheit Mittel mit Sicherheitsfunktion zur Erkennung von Fehlern beinhaltet, wobei jedem Fehler eine Überwachungsroutine zugeordnet ist, wobei eine Mehrzahl von Überwachungsroutinen zur Verfügung steht und den Mitteln mit Sicherheitsfunktion eine Abschaltmatrix zugeordnet ist, welche nach Fehlern unterteilt ist, wobei weitere Mittel enthalten sind, welche entsprechend der vorhandenen Fehler in der Abschaltmatrix wenigstens eine der Überwachungsroutinen abhängig von wenigstens einer ersten Bedingung aus der Mehrzahl von Überwachungsroutinen auswählen, wobei die Abschaltmatrix weiterhin verschiedene Abschaltstrategien enthält und dass die weiteren Mittel bei Erkennung wenigstens eines Fehlers durch die ausgewählte Überwachungsroutine abhängig von wenigstens der ersten und/oder wenigstens einer zweiten Bedingung eine der Abschaltstrategien im Netzwerk ausführen, wobei wenigstens eine Steuereinheit im Netzwerk abgeschaltet wird.

10. Programm oder Programmprodukt, welches ausgeführt durch wenigstens eine Steuereinheit eines Netzwerkes ein Verfahren nach einem der Ansprüche 1 bis 7 durchführt.

20.12.00 Sy/Hx

ROBERT BOSCH GMBH, 70442 Stuttgart

# Verfahren und Vorrichtung zur Überwachung und Abschaltung von Steuereinheiten in einem Netzwerk und Netzwerk

Zusammenfassung

Verfahren zur Überwachung von Steuereinheiten in einem Netzwerk, wobei jede Steuereinheit eine Sicherheitsfunktion zur Erkennung von Fehlern beinhaltet, wobei jedem Fehler eine Überwachungsroutine zugeordnet ist und eine Mehrzahl von Überwachungsroutinen zur Verfügung steht, wobei der Sicherheitsfunktion eine Abschaltmatrix zugeordnet ist, welche nach Fehlern unterteilt ist, wobei entsprechend der vorhandenen Fehler der Abschaltmatrix wenigstens eine der Überwachungsroutinen abhängig von wenigstens einer ersten Bedingung aus der Mehrzahl von Überwachungsroutinen gewählt wird, wobei die Abschaltmatrix verschiedene Abschaltstrategien enthält und dass bei Erkennung wenigstens eines Fehlers durch die Überwachungsroutine abhängig von wenigstens der ersten und/oder wenigstens einer zweiten Bedingung eine der Abschaltstrategien im Netzwerk ausgeführt wird, wobei wenigstens eine Steuereinheit im Netzwerk abgeschaltet wird.

(Figur 3)

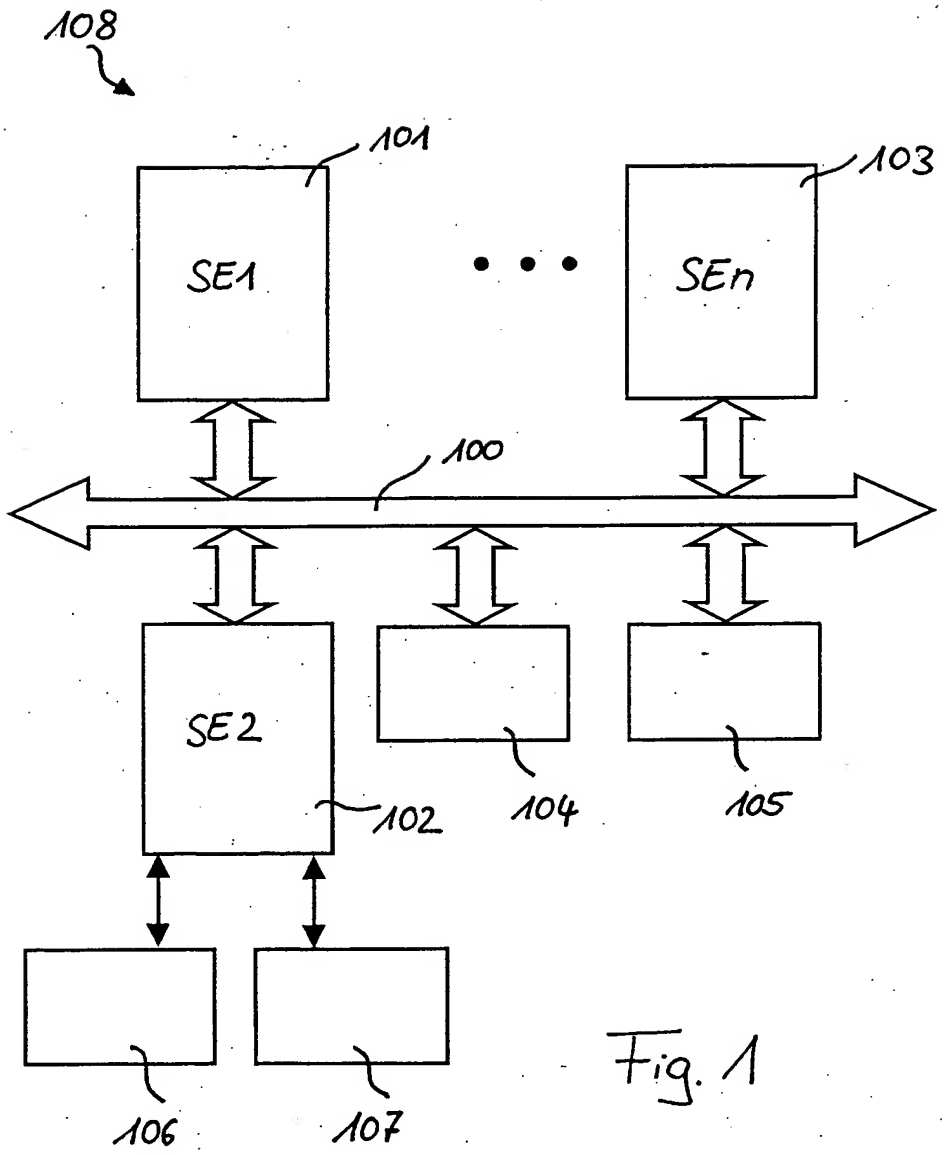


Fig. 1

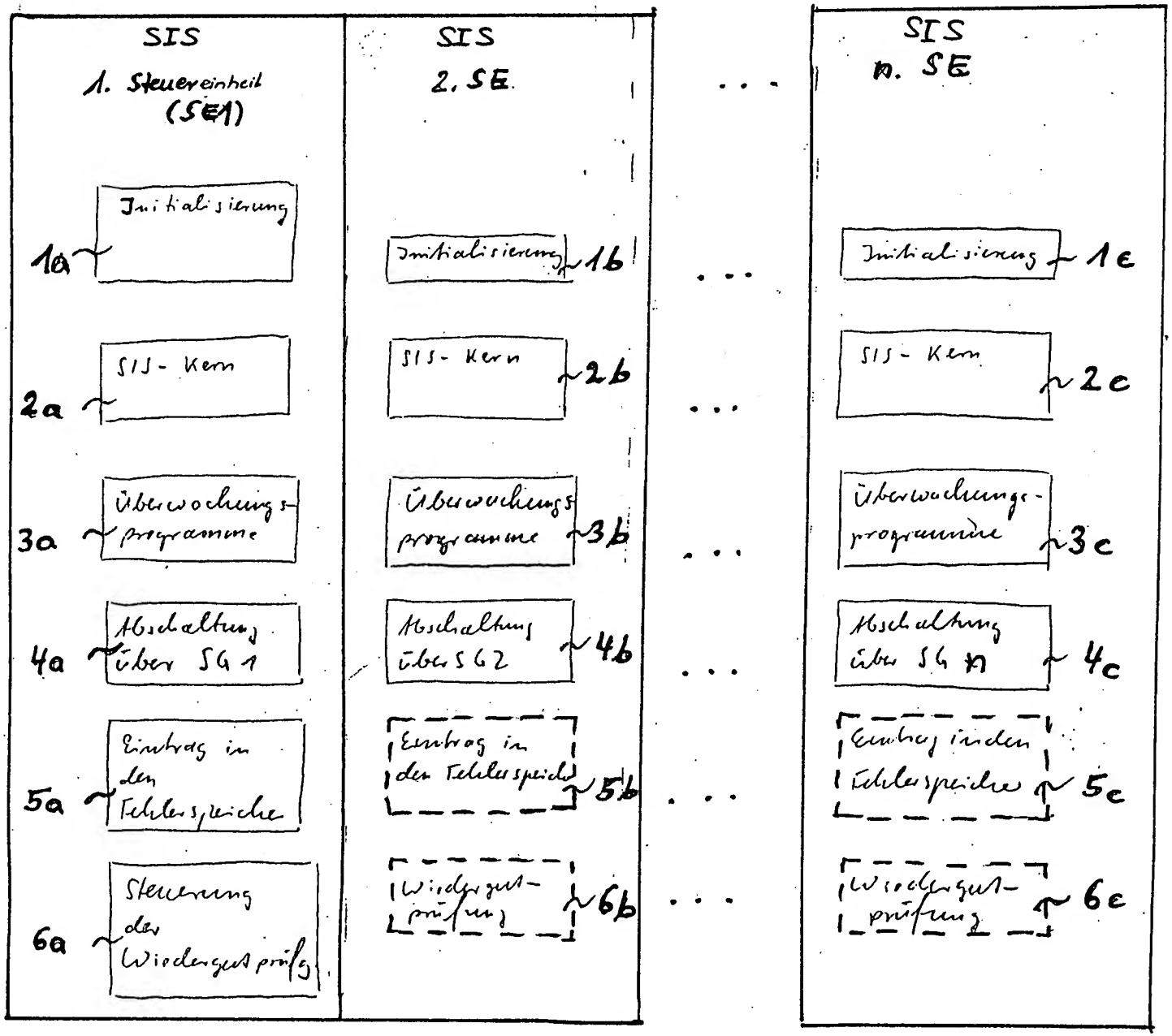
SIS
1. Steuereinheit (SE1)
SIS
2. SE
SIS
n. SE
1a
Initialisierung
1b
Initialisierung
1c
Initialisierung
2a
SIS - Kern
2b
SIS - Kern
2c
SIS - Kern
3a
Überwachungs-programme
3b
Überwachungs-programme
3c
Überwachungs-programme
4a
Abschaltung über SG 1
4b
Abschaltung über SG 2
4c
Abschaltung über SG n
5a
Eintrag in den Fehlerspeicher
5b
Eintrag in den Fehlerspeicher
5c
Eintrag in den Fehlerspeicher
6a
Steuerung der Wiedergutprüfg.
6b
Wiedergut-prüfung
6c
Wiedergut-prüfung

Fig. 2

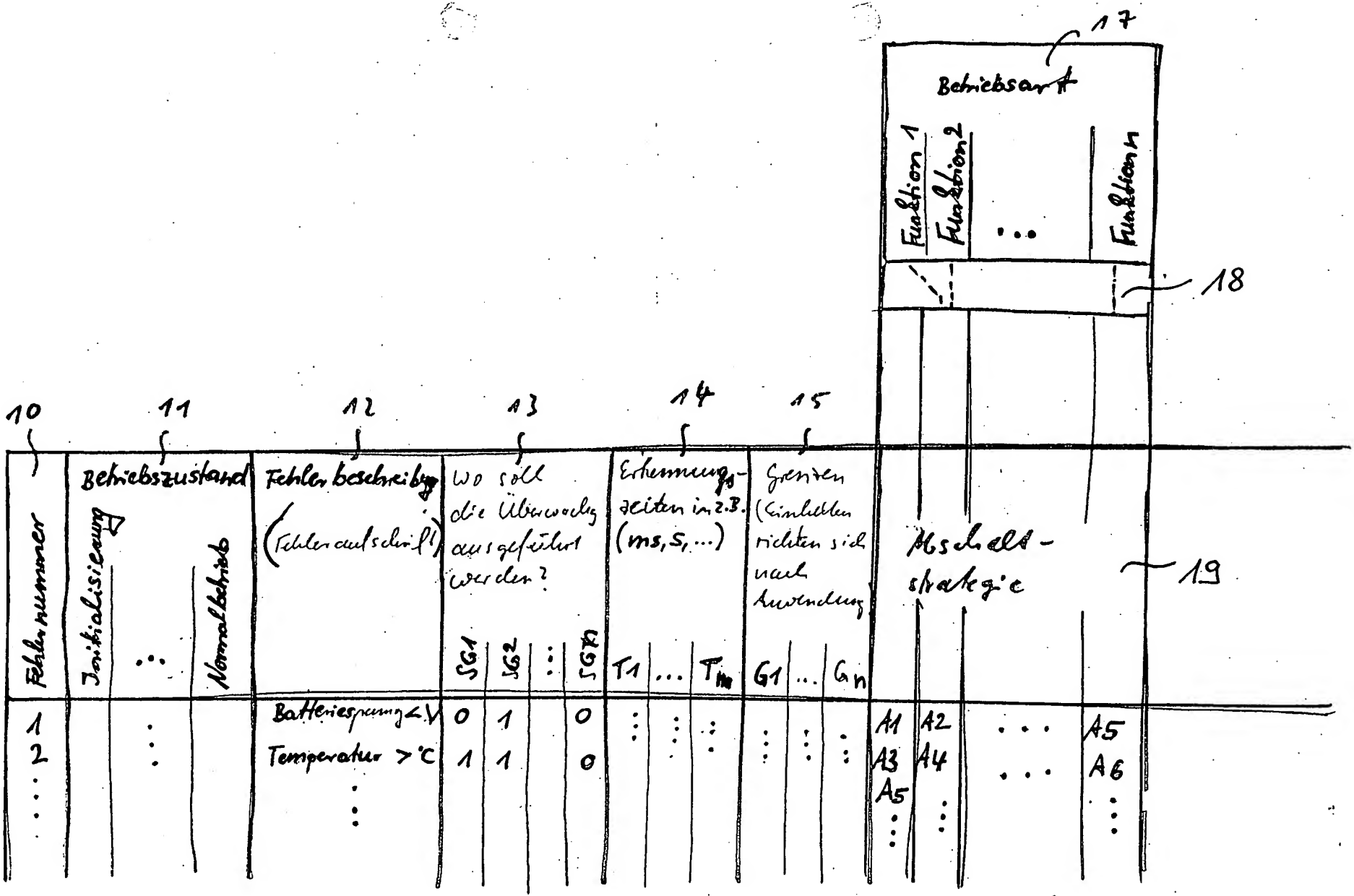
17
Betriebsart
Funktion 1
Funktion 2
...
Funktion n
18
10
11
12
13
14
15
Fehlernummer
Betriebszustand
Initialisierung
...
Normalbetrieb
Fehlerbeschreibung
(Fehlereintrag)
wo soll die Überwachung ausgeführt werden?
SG1
SG2
...
SGn
Ansprechzeiten in z.B. (ms, s, ...)
T1
...
Tm
Grenzen (Einheiten richten sich nach Anwendung)
G1
...
Gn
Abschaltstrategie
19
1
2
...
Batteriespannung < V
Temperatur > °C
0
1
1
1
0
0
A1
A2
A3
A4
A5
A6
5/3
K4004

Fig 3